

2024 GIFCT Annual and Transparency Report



GIFCT
Global Internet Forum
to Counter Terrorism

Preventing terrorists and violent extremists from exploiting digital platforms

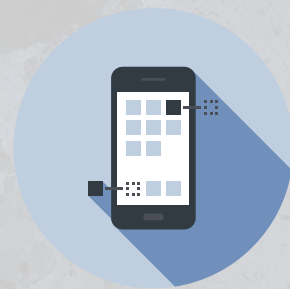
The Global Internet Forum to Counter Terrorism brings together the technology industry, government, civil society, and academia to foster collaboration and information sharing to counter terrorist and violent extremist activity online.



33
member
tech platforms



32
countries
represented in
2024 Working Groups



≈2.3
million
hashes in the
hash-sharing database

Table of Contents

Executive Summary	4
Introduction	6
Letter from Executive Director, Naureen C. Fink	7
Letter from 2024 Operating Board Chair, Courtney Gregoire	9
Letter from Independent Advisory Committee Chair, Ghayda Hassan	11
Membership	13
2024 Membership Updates	14
GIFCT's Value Proposition	17
Becoming A GIFCT Member / Join GIFCT	18
Hash Sharing	19
The Hash-Sharing Database	19
Composition of the Hash-Sharing Database	20
Taxonomy for the Hash-Sharing Database	21
Labels for the Hash-Sharing Database	21
Member Hash Feedback	23
Hash Removals	23
Reviewing and Refining the Hash-Sharing Database	24
Incident Response	25
The Incident Response Framework	25
Types of Response	25
2024 Activations	27
Hashing and the Incident Response Framework	28
Reviewing and Refining the Incident Response Framework	28
Research and Analysis	29
Global Network on Extremism and Technology	29
GNET Publications	30
GIFCT Knowledge Products	32
Knowledge Exchange and Collaboration	33
Events	33
Global Multi-Stakeholder Forum	33
Regional Workshops	34
Canada Center Mega Week	36
External Engagements	37
United Nations, New York	38
2024 Annual Member Forum	38
GNET Conference	39
GNET Webinars	39
2024 Working Groups	39
Human Rights	43
2024 Developments	43
Financials	44
Financial Support and Contributions	44
2024 Expenses	45
Improving GIFCT's Readiness in 2025	47

Executive Summary

In 2024, GIFCT delivered for its members and stakeholders through enhanced collaboration, improved resources, and strengthened connections between industry and global expertise, supporting collaborative efforts to address terrorism and violent extremism online.

GIFCT welcomed six new platforms – BIMeta, Bitly, Patreon, Streamable, Vimeo, and Yahoo – broadening the diversity of its membership and the tech stack GIFCT supports. This expansion to **33 members** reflects GIFCT's continued commitment to cross-platform collaboration as the online threat landscape grows more complex and globally dispersed.

In 2024, GIFCT developed frameworks to launch its in-house Membership Advisory Program (MAP) to support potential member platforms and those already in the membership pipeline. In planning for this internal mentorship process, GIFCT created processes, timelines, and staff allocations to support platforms working toward full membership. To better facilitate knowledge exchange among members and enhance access to existing resources, GIFCT updated the **GIFCT Member Resource Guide**, a key tool for platforms seeking to strengthen their policies and practices related to countering terrorism and violent extremism.

In 2024, GIFCT's "Tech team" **rebranded as the Trust and Safety Solutions team** to better align with the needs of its member tech platforms. This shift reflects its commitment to better supporting trust and safety practitioners and clarifying its role as a collaborative partner in countering online threats. Core tools like the hash-sharing database (HSDB) and Incident Response Framework (IRF) remain central and are now positioned within a broader and evolving suite of practical trust and safety solutions.

Terrorists and violent extremists also made renewed efforts in 2024 to exploit digital platforms. In 2024, **GIFCT and its members activated the IRF seven times** in response to terrorist and mass violence events with a significant online aspect, and **increased the number of distinct items in the HSDB to 408,000** images, videos, and texts.

In 2024, GIFCT expanded its suite of knowledge products to better serve its key stakeholder communities, publishing in-depth resources to offer more targeted support addressing the specific needs of its members. Its academic research arm, **the Global Network on Extremism and Technology (GNET)**, published 120 GNET reports, **62 of which highlighted attempts by terrorists or violent extremists to exploit GIFCT member platforms**.

GIFCT also strengthened its global engagement in 2024. In **Singapore**, GIFCT cohosted with Microsoft a Global Multi-Stakeholder Forum and reinforced its collaborative approach to identifying regional and cross-platform solutions. **GIFCT's first Latin American multi-stakeholder workshop**, hosted in Rio de Janeiro in partnership with the Industry Federation of the State of Rio de Janeiro (Firjan), deepened its understanding of regional threats, trends, and opportunities on the continent. In **Stockholm**, GIFCT hosted a multi-stakeholder workshop at the Nordic Democracy Forum to assess cross-sector challenges and identify opportunities for stronger collaboration. Alongside the opening of the **United Nations General Assembly session in New York**, GIFCT convened three side events with key partners to highlight the current state of play in online counter terrorism efforts and explore future opportunities for collaboration among stakeholders in industry, academia, and policy. This included events focused

on emerging technologies, youth intervention, and sanctions within the tech sector.

2024 also saw the **fourth annual GNET Conference and GNET webinars**, where experts from across sectors shared insights and learnings from the intersection of tech and counter terrorism. To cap off the year, GIFCT's **Annual Member Forum** offered a dedicated space for its industry members to share insights, shape priorities for 2025, hear from its IAC, and ensure its future work remains responsive to member industry needs and emerging risks.

GIFCT's Working Groups continued to deliver meaningful outputs aligned with its mission to prevent terrorist and violent extremist exploitation of digital platforms. In 2024, **Working Groups produced guidance to evolve the HSDB, reviewed the IRF and shared suggestions that are helping to inform improvements being made to the framework in 2025**,¹ and created a community of practice and a set of **resources for gaming platforms**, including a literature review on gaming and extremism and best practices for safety-by-design.

GIFCT also made continued progress towards meeting its **human rights goals in 2024** by collaborating with a broader group of UN bodies and international organizations, hosting a human rights workshop for member companies, and developing the MAP to include more human rights consulting and support for members.

GIFCT's mission is global, and no single sector can alone address these threats. As such, GIFCT is proud to work with industry, government, and civil society partners to ensure diverse worldwide perspectives inform its work. GIFCT remains committed and reaffirms its goal to work collaboratively, transparently, and in a manner that fosters respect for human rights to prevent terrorists and violent extremists from exploiting digital platforms.

.....
¹ https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-IRWG_Report-1.1.pdf

Introduction

The [Global Internet Forum to Counter Terrorism \(GIFCT\)](#)² is a unique tech-led nonprofit organization dedicated to preventing terrorists and violent extremists from exploiting digital platforms.

Having grown from an initial group of four founding members, GIFCT now convenes more than [30 member technology platforms](#)³ and fosters collaboration and dialogue with diverse stakeholders – including industry, government, civil society, and academia – to advance collective counter terrorism efforts through four key tools. These include the hash-sharing database (HSDB) and Incident Response Framework (IRF), as well as a platform for cross-industry knowledge sharing and collaboration. Through its academic arm, the Global Network on Extremism and Technology (GNET), GIFCT connects global experts with the tech sector, providing critical insights into emerging threats and trends shaping digital safety and supporting industry actors in adapting to these evolving trends.

Established in 2017 to address the exploitation of social media platforms by terrorist organizations such as ISIS, GIFCT's founding members saw an even greater need for the tech industry to marshal its collective capacity to render terrorists and violent extremists ineffective online following the 2019 terrorist attacks in Christchurch, New Zealand.

Today, GIFCT operates as an independent nonprofit organization conducting programmatic, technological, and strategic initiatives with its growing community of diverse tech platform members. An Operating Board currently comprising Meta, Microsoft, and YouTube is advised by an [Independent Advisory Committee \(IAC\)](#)⁴ composed of representatives from civil society, academia, government, and intergovernmental organizations. Through a range of regional multi-stakeholder workshops, virtual and in-person events, and via GNET, GIFCT continues to foster worldwide engagement and collaboration alongside feedback and knowledge sharing, and encourages industry representatives worldwide to join as GIFCT members.

.....
² <https://gifct.org/>

³ <https://gifct.org/membership/>

⁴ <https://gifct.org/governance/>

Letter from Executive Director, **Naureen C. Fink**

In many ways, 2024 was a transformative year for GIFCT, marked by the organization's maturation through an expanded and diversified membership, new regional partnerships worldwide, and the strengthening of a multi-stakeholder community to inform and shape tech solutions and responses to evolving terrorist threats.

We welcomed new team members specializing in Trust and Safety Solutions and Incident Response while laying the groundwork for additional roles and functions to better support our members and achieve our goals. We reviewed and assessed many of our key tools and processes and welcomed feedback from our member companies, our Independent Advisory Committee (IAC), and our Working Groups on Incident Response and Hash Sharing. Following up on those discussions and recommendations remains a key priority of the organization.

GIFCT's unique role in bringing together leaders at the intersection of technology and counter terrorism was highlighted through the development and strengthening of numerous relationships with regional partners and experts in Latin America, the Middle East, Africa, and the Nordic and Asia-Pacific regions. The resulting global networks and connections to researchers and expertise across diverse geographies through our academic research arm, the Global Network on Extremism and Technology (GNET), ensure that our members and partners have access to critical research and insights that can help industry identify evolving harms and adapt responses.

We remain firmly committed to multi-stakeholder engagement, demonstrated in the Global Multi-Stakeholder Forum co-hosted with Microsoft in Singapore, as well as our regional multi-stakeholder convenings in Brazil and Sweden, and engagement in TrustCon, the Terrorism and Social Media conference, the Aqaba Process, Raisina Dialogue, and with international organizations including the United Nations, the Organization for Security and Co-operation in Europe, and the European Union. Through these international engagements, we have sought to connect with prospective members, industry associations, and experts to support the diversification of GIFCT's membership. We were pleased to welcome six new members in 2024, bringing the total to 33.

I am deeply grateful to our Operating Board and the IAC for their commitment to GIFCT's mission and their ongoing support. The governance changes adopted by the Board in summer 2024 institutionalize important opportunities to expand the Board and integrate diverse perspectives and experiences from across the tech sector while ensuring a more sustainable future for GIFCT. The new Strategic Plan developed by GIFCT for 2025–2027 and adopted by the Board – with inputs from GIFCT's IAC and reflecting feedback from member companies and stakeholders throughout the year – creates a roadmap for the organization to ensure that our trajectory each year aligns with the key priorities and goals that have been set out.

I would like to extend my thanks and appreciation to Microsoft, our 2024 Operating Board Chair, for their leadership and the trust and support they have offered throughout the year. We very much look forward to working with YouTube as our 2025 Board Chair in advancing our strategic goals. I would also like to extend my thanks to the IAC and its Chair, Ghayda Hassan, and Vice Chair, Jonathan Russell, for the invaluable advice and input that have shaped our workstreams and efforts throughout the year.

Looking ahead to 2025, I am excited to build on many of the transformations instituted this year.

With the continued collaboration and support of our stakeholder community, I am confident GIFCT will be better positioned to support its members and partners in addressing evolving threats, trends, and opportunities. I am ever grateful to GIFCT's team for their constant dedication, vigilance, and commitment to preventing terrorists and violent extremists from exploiting digital platforms.

Thank you for your dedication to our shared mission.

A handwritten signature in black ink, appearing to read 'Naureen C. Fink', with a stylized, flowing script.

Naureen C. Fink
Executive Director, GIFCT

Letter from 2024 Operating Board Chair, Courtney Gregoire

As the 2024 Chair of the Operating Board, I am proud to report that – in the face of rapid technological change and geopolitical uncertainty – GIFCT has not wavered in its commitment to our shared mission of combating terrorism and violent extremism online while upholding fundamental human rights.

In late 2023, the Operating Board asked ourselves how we could deliver more effective and more impactful solutions for members. Through our collective efforts, we made remarkable progress toward that goal in 2024.

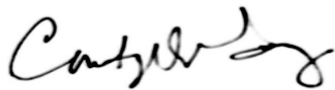
- **We renewed our commitment to building out the global nature of GIFCT's work and its membership.** In June, we held GIFCT's Global Multi-Stakeholder Forum in Singapore – the first such forum outside North America – with the express purpose of enhancing diverse multi-stakeholder participation. The forum reinforced the importance of cross-sector collaboration between governments, civil society, technology platforms, and academia in combating terrorism and violent extremism online. It also underscored GIFCT's commitment to fostering awareness of different regional contexts and challenges. I'm grateful for the engagement of GIFCT's Independent Advisory Committee (IAC) and other forum participants, whose practical insights are critical to GIFCT's ability to continue delivering on its mission.
- **We strengthened our capacity to adapt to changes in technology and the threat landscape.** Last year, GIFCT embraced a strategy centered on enabling the development of new safety tools and guidance that respond to evolving technologies, in particular generative AI. Similarly, GIFCT's multidisciplinary working groups focused their work on practical solutions that will benefit the broader online ecosystem.
- **We grew as a community of technology platforms working to improve the broader ecosystem.** GIFCT added six member platforms in 2024, expanding its total to 33. The addition of BIMeta, Bitly, Patreon, Streamable, Vimeo, and Yahoo reflects GIFCT's dedication to growing a diverse and globally representative network. This diversity is crucial, as it allows GIFCT to address threats across various platforms and technologies, from social media and livestreaming to gaming, messaging, and cloud services.
- **We remained ready to respond to terrorist or violent extremist incidents with online dimensions.** GIFCT continued to provide valuable incident-response capabilities to its members. It invoked formal incident-response mechanisms following four separate terrorist or violent extremist events, and it supported its members by monitoring and disseminating information on scores of others.
- **We positioned GIFCT for the future through significant changes to the organization's governance.** Recognizing the need for greater accountability and participation, the Board revised GIFCT's bylaws and adopted a consolidated set of membership and governance policies. These changes are designed to foster a more inclusive and transparent organization, encouraging broader participation from members and stakeholders.

At Microsoft, we're very proud to be part of an organization that has delivered concrete progress on such an important, urgent issue. GIFCT occupies a truly unique position, delivering solutions by

technology platforms for the broader online ecosystem. I want to extend my heartfelt thanks to GIFCT's dedicated staff, members, and stakeholders for their hard work and commitment. I am also grateful to YouTube for taking over the role of GIFCT Board Chair in 2025 and working to ensure that GIFCT will continue to thrive and evolve.

Combating terrorist and violent extremist use of digital technologies will always be a challenge, but GIFCT is better equipped than ever to support its members in tackling that challenge while safeguarding fundamental rights. I look forward to continuing this work with GIFCT, its members, the IAC, and our other partners and stakeholders.

Warmly,

A handwritten signature in black ink, appearing to read 'Courtney Gregoire', with a stylized, flowing script.

Courtney Gregoire

Vice President and Chief Digital Safety Officer, Microsoft

Letter from Independent Advisory Committee Chair, *Ghayda Hassan*

The years 2024 and early 2025 have been marked by significant challenges for those working to prevent and counter terrorist and violent extremist incidents and content. Offline, we continue to witness horrific extremist violence, including genocide, mass attacks on civilian populations worldwide, and the strengthening of totalitarian regimes, militias, and violent extremist groups.

Online, we are observing increasing fragmentation of the tech sector, the hybridization of extremist narratives, and the mass production and diffusion of terrorist and violent extremist content (TVEC), with heightened risk of exposure for young, vulnerable, or affected audiences. Malicious actors are adapting rapidly and targeting increasingly younger populations with nihilistic narratives – connected to adult-driven conflicts, economic instability, and the climate crisis – and pushing them toward extreme forms of self-harm.

Furthermore, the digital landscape is undergoing deep transformation due to the race for generative AI, gaming, deepfake technologies, gaps in platform policies, and, in some cases, loosening of regulations on TVEC. The potential for these technologies to be used to produce “lawful but awful” content – hate speech, propaganda, and misinformation – poses real threats to social trust and our shared sense of humanity.

It is troubling to see the continued status quo as governments, civil society, and the tech industry at large fall short of making bold decisions and working truly hand in hand. The future of humanity demands effective protection for the most impacted – children, youth, and marginalized communities – from these harms.

In this context, the work GIFCT has undertaken in 2024 has been critical.

GIFCT and its Operating Board implemented policy and structural adjustments, expanded global outreach, and proactively engaged with evolving threat environments. GIFCT simplified its policies to become a stronger, more agile organization, relying on the proactive participation of all its members. In its ongoing push for globalization, GIFCT expanded its membership to 33 and streamlined its Working Groups to review tools and deliver tangible outputs in three key areas:

- The hash-sharing database (HSDB), which is clarifying elements of its inclusion criteria and providing new opportunities for members to collaborate;
- The Incident Response Framework (IRF), which is improving in both scope and agility to more effectively address an increasingly global threat landscape; and
- New tools and strategies for gaming safety, which aim to enhance protections in that rapidly evolving space.

GIFCT also successfully engaged stakeholders and members globally through events in Singapore, at the United Nations General Assembly, and via online platforms. Notably, GIFCT’s full ownership of the member onboarding process will enhance transparency and, we hope, improve efficiency in expanding a diverse membership beyond subsidiary platforms.

It is essential for tech platforms to continue working with GIFCT and participating in its leadership to anticipate future harms that cross geographies and populations. Now more than ever, efforts to address TVEC at its core must remain transparent and firmly grounded in principles of human rights.

As I approach the end of my three-year chairpersonship and reflect on this journey, it is clear that the Independent Advisory Committee (IAC), the Operating Board, and GIFCT have come a long way from their early formative years. These bodies are now mature, constructive, and rooted in foundational principles and mechanisms that foster collaboration, dialogue, accountability, and meaningful action. This unique tripartite model within the tech governance landscape has demonstrated real value in shaping both policy and operational priorities.

Looking ahead, I am confident the IAC will continue its mission of promoting good governance, diversity, and growth, and that GIFCT will meet its strategic objectives with strength and transparency. The IAC will keep enhancing GIFCT's value to members and identifying creative ways to engage tech platforms – including those at higher risk and with less interest in regulation – as well as relevant adjacent organizations. This is essential to reflect a truly global reach. The IAC will also continue advising on emerging trends and deepening engagement with governments, civil society, and affected global communities.

As TVEC drivers, actors, and activities are transnational, networked, and intertwined with broader political and structural harms, GIFCT's success will depend on its ability to remain well resourced, equipped with cutting-edge expertise and best practices, and guided by human rights standards. In turn, GIFCT and its IAC must continue to be entrusted with the infrastructure, investment, and cross-sector partnerships needed to lead effectively.

Sincerely,



Ghayda Hassan

Chair, Independent Advisory Committee

Membership

At its inception, GIFCT had four founding members. At the end of 2024, [GIFCT members](https://gifct.org/membership/)⁵ included 33 platforms representing diverse digital solutions and geographic origins.

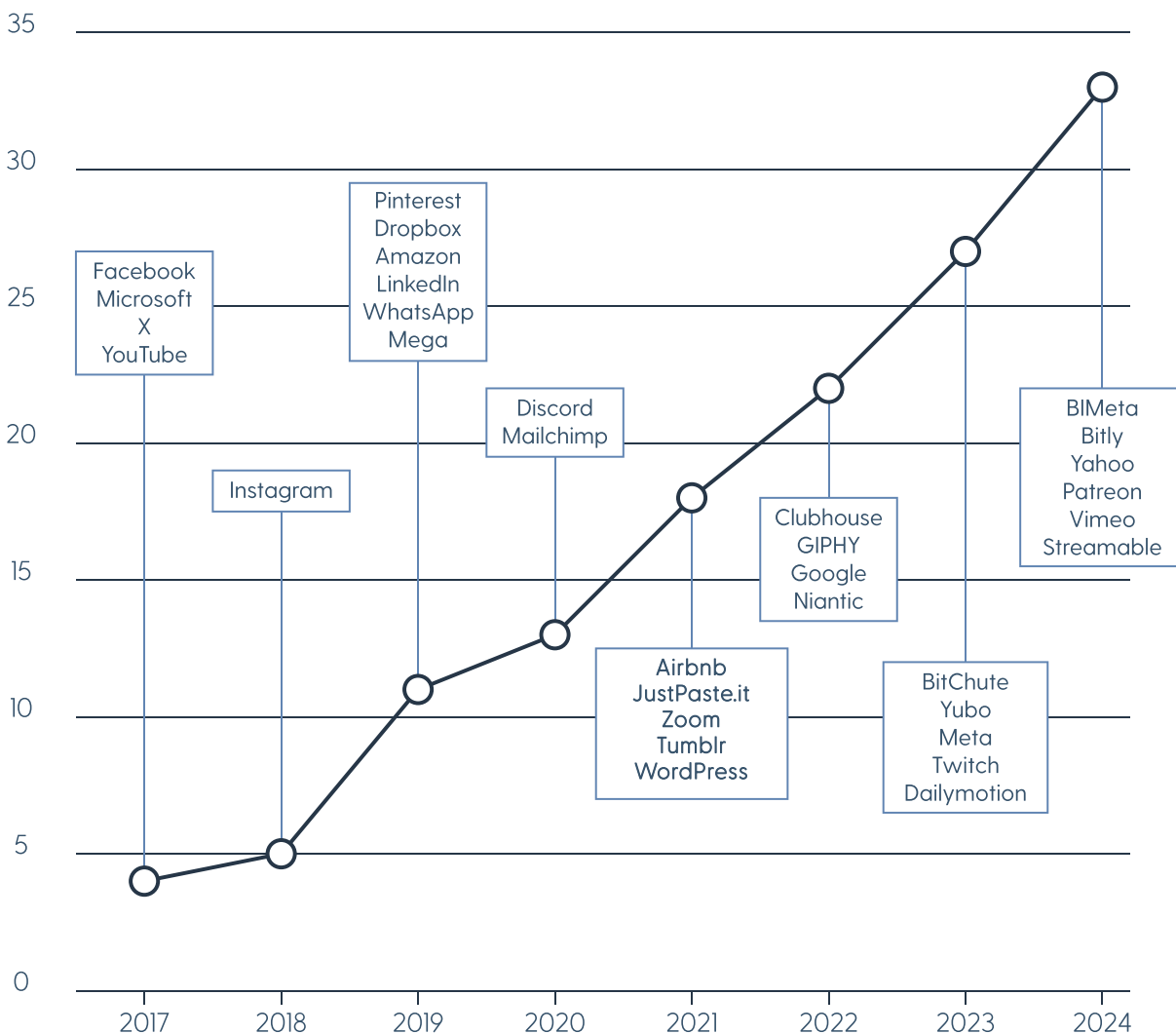


Figure 1: GIFCT members over time

Each member that joins GIFCT brings new technology, experience, and expertise to the table, expanding and strengthening its collective capacity. Diversifying GIFCT's membership ensures a range of voices and global perspectives are represented, and provides additional opportunity to address threats across more platforms and technologies.

.....
⁵ <https://gifct.org/membership/>

GIFCT Members

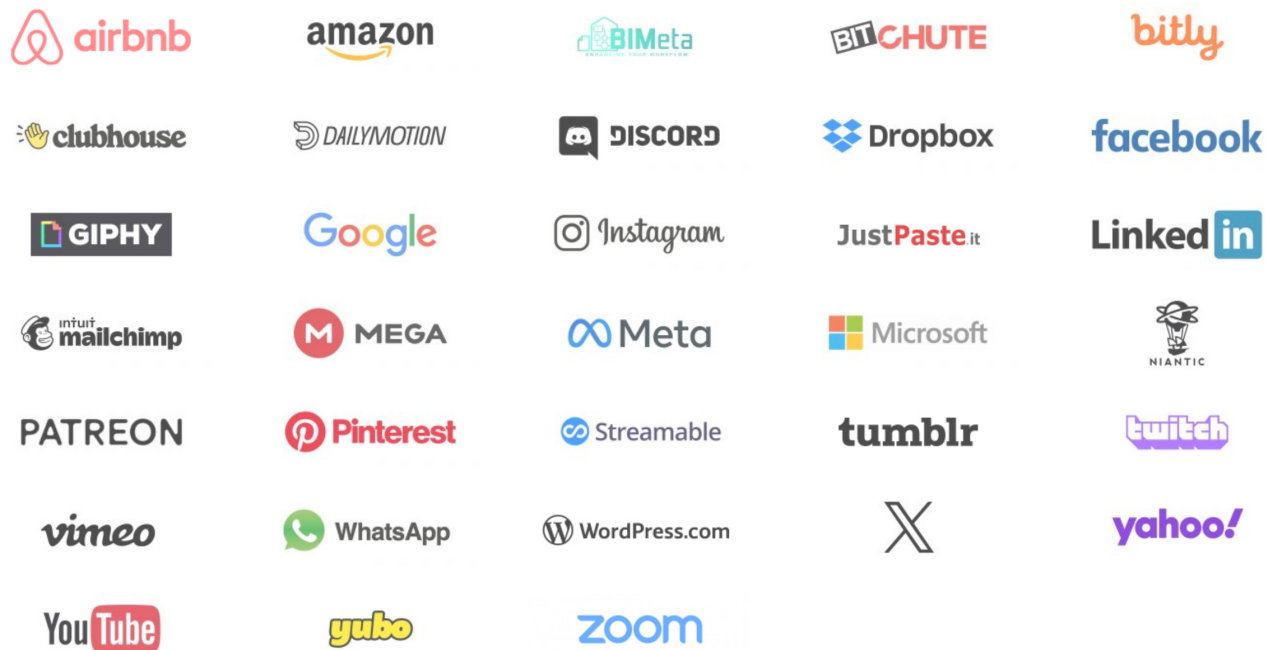


Figure 2: GIFCT member companies

2024 Membership Updates

Six platforms became GIFCT members in 2024 – BIMeta, Bitly, Yahoo, Patreon, Vimeo, and Streamable. GIFCT's newest members help further advance its mission through representing both smaller platforms and larger platforms with global impact. These new members strengthen GIFCT's reach into key areas, including social media, video streaming, image sharing, URL shortening, monetization and finance, and web searching. Adding these new member platforms continues to diversify GIFCT's membership and provides it with an even more comprehensive view of the ever-evolving threat landscape.

2024 also saw membership applications from several new platforms and the continued mentorship of prospective members as they work toward meeting GIFCT eligibility requirements.

Patreon was built for creators – not for enabling or facilitating violence and extremism. We take swift action to remove violative works, but we recognize that we need to work across online platforms to maximize our impact and proactively curb the spread of this dangerous content. GIFCT provides a structured and action-oriented space for community-driven dialogue, allowing us to discuss best practices, address shared challenges, and strengthen our existing trust and safety efforts. As a new member of GIFCT, we look forward to continuing to do our part in keeping the internet safe for creators and fans on – and off – Patreon.

Eric Han, Vice President of Trust and Safety, Patreon

GIFCT members provide different types of services, including:

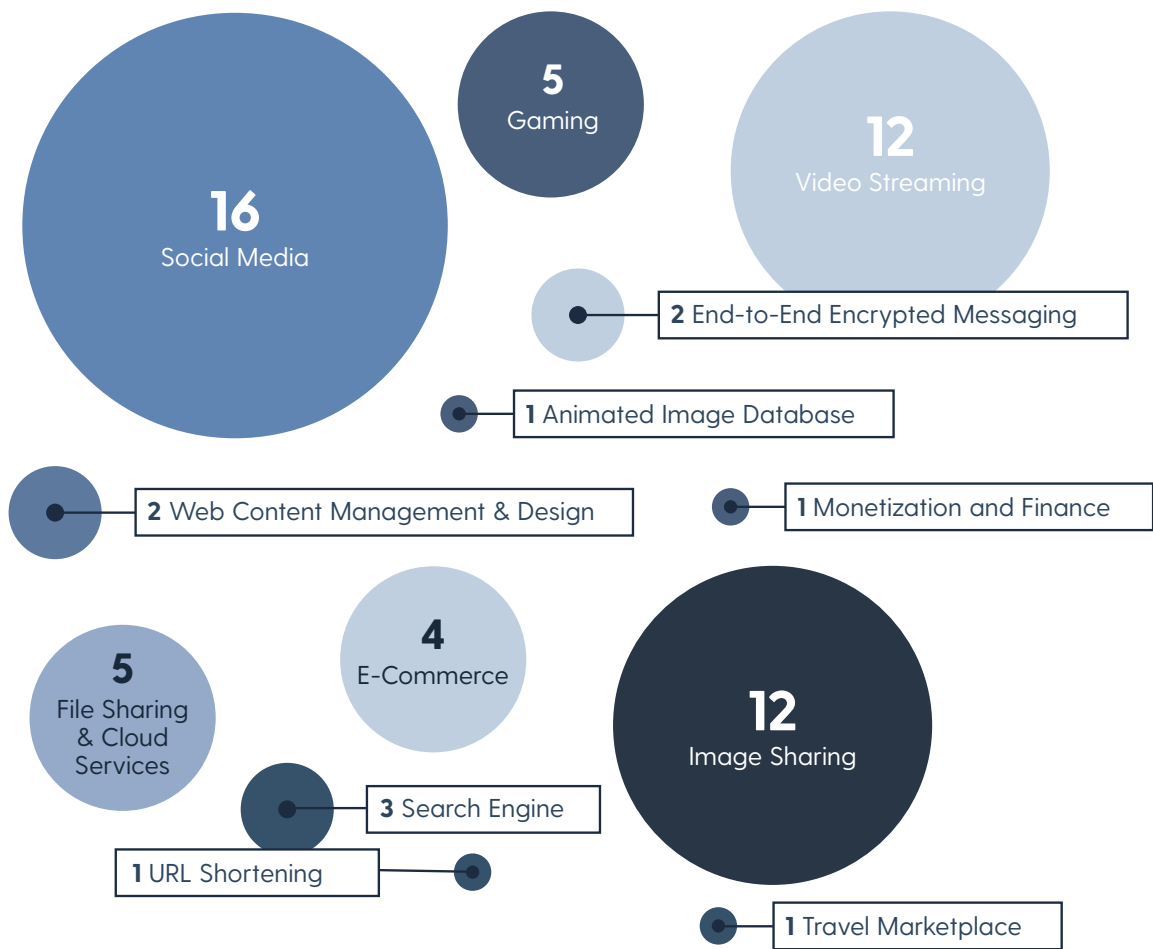


Figure 3: Services of GIFCT member companies

In 2024, GIFCT also laid the groundwork for the new **Membership Advisory Program (MAP)**, which, starting in 2025, will enable GIFCT to manage the entirety of membership activities. Before the program's comprehensive redesign in the third quarter of 2024, GIFCT partnered with Tech Against Terrorism and Business for Social Responsibility (BSR) to advise several platforms on fulfilling their membership criteria. In collaboration with BSR, GIFCT supported 11 platforms with human rights reviews, delivered a virtual human rights workshop for member companies, and produced human rights-focused materials for current and prospective GIFCT members.

GIFCT greatly values the commitment of members and applicants to the membership criteria. Through the course of working towards GIFCT membership in 2024, companies advanced in key ways:

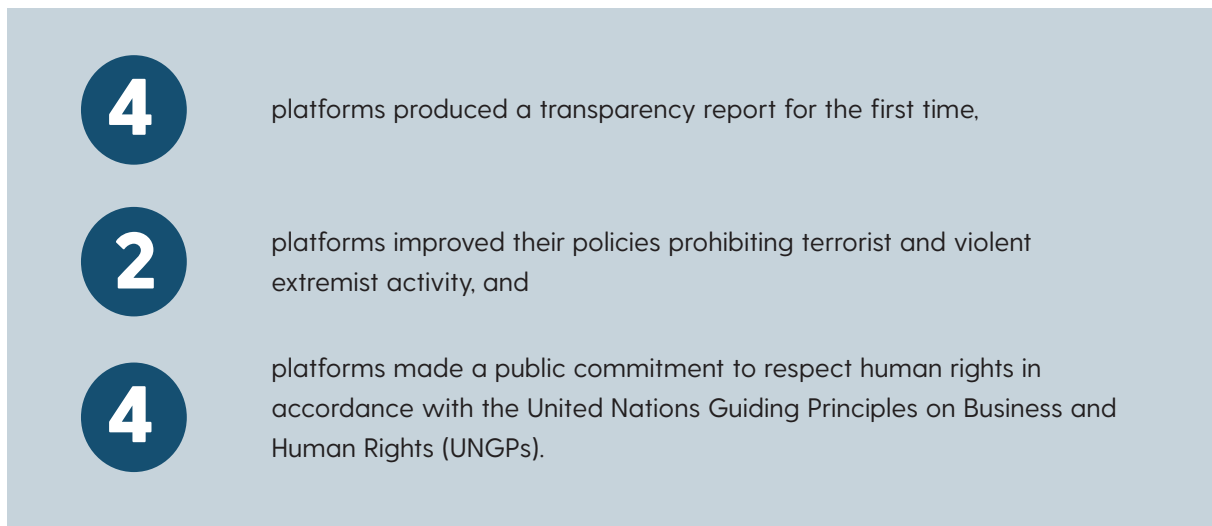


Figure 4: GIFCT prospective member advancements

In 2024, GIFCT also revised the [GIFCT Member Resource Guide](https://gifct.org/resource-guide/)⁶ – an essential tool designed to help platforms enhance their counter terrorism and violent extremism policies and practices. The updated guide features enhanced functionality and new content, including filterable resources from member companies across platform types, revised appendices, and expanded information on GIFCT's tools, Working Group outputs, and membership support.

GIFCT continued to seek feedback and engagement from member tech platforms and the broader multi-stakeholder community to strengthen and improve the tools and resources it provides. Member feedback, Working Group findings, and insights from its multi-stakeholder engagements are central to informing GIFCT's work and delivering on its mission.

.....
⁶ <https://gifct.org/resource-guide/>

GIFCT's Value Proposition

Being a GIFCT member means having access to a global information network built specifically to strengthen tech platforms' capacity to counter terrorist and violent extremist activity online.

Once applicants have met its membership criteria, member platforms receive:



Figure 5: GIFCT member benefits

GIFCT connects member platforms with a suite of technical solutions, tools, and resources to strengthen their efforts against terrorist and violent extremist activity online. This includes access to technical and cross-platform information-sharing solutions, including the HSDB and IRF, and bespoke resources tailored to emerging threats and platform-specific needs. Members also receive briefings from international subject matter experts and regular opportunities to enhance situational awareness and foster collaboration through [global convenings](https://gifct.org/global-summits/)⁷ and knowledge-sharing forums, such as GIFCT's [Working Groups](https://gifct.org/working-groups-landing-page/).⁸

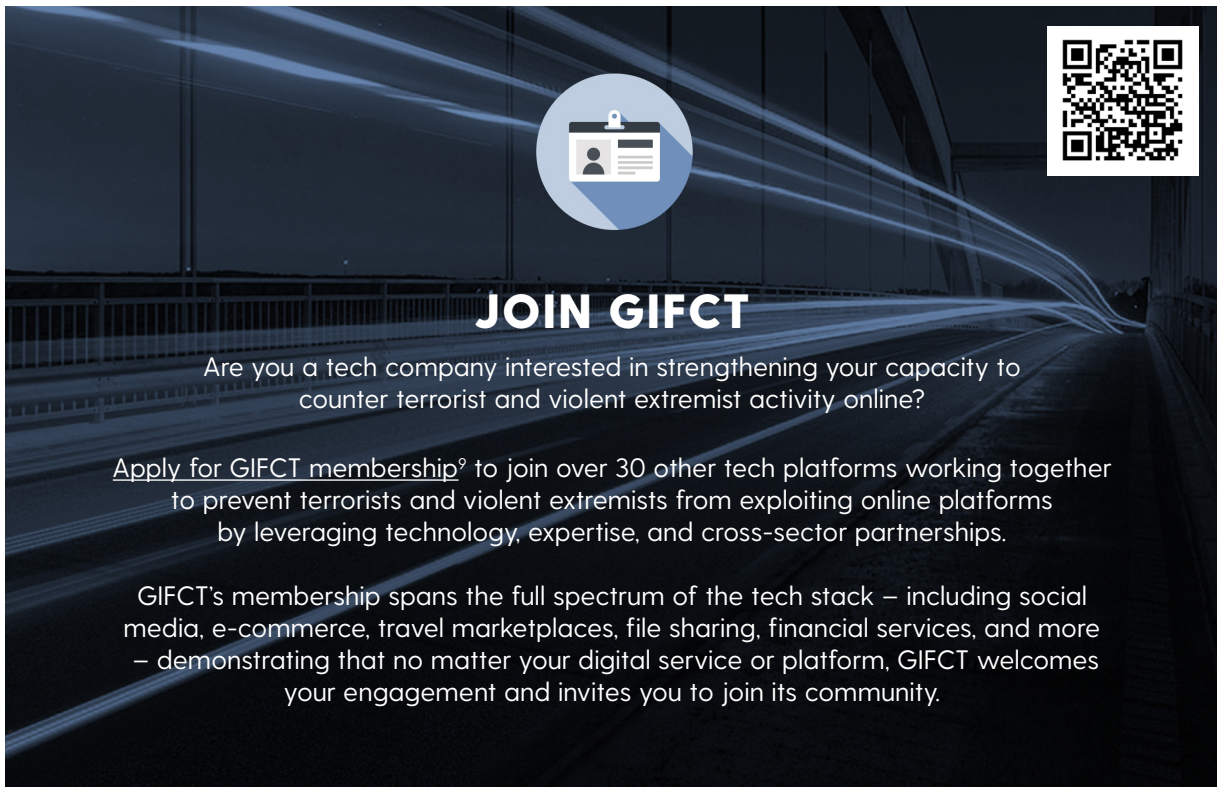
7 <https://gifct.org/global-summits/>

8 <https://gifct.org/working-groups-landing-page/>

Becoming A GIFCT Member

Digital platforms seeking to join GIFCT must meet specific membership criteria, ensuring alignment with its mission and values. These include:

- Terms of service, community guidelines, or other publicly available policies that explicitly prohibit terrorist and/or violent extremist activity.
- The ability to receive, review, and act on reports of activity that is illegal and/or violates terms of service and user appeals.
- A desire to explore new technical solutions to counter terrorist and violent extremist activity online.
- Regular, public data transparency reports.
- A public commitment to respect human rights in accordance with the UNGPs.
- Support for expanding the capacity of civil society organizations to challenge terrorism and violent extremism.



JOIN GIFCT

Are you a tech company interested in strengthening your capacity to counter terrorist and violent extremist activity online?

Apply for GIFCT membership⁹ to join over 30 other tech platforms working together to prevent terrorists and violent extremists from exploiting online platforms by leveraging technology, expertise, and cross-sector partnerships.

GIFCT's membership spans the full spectrum of the tech stack – including social media, e-commerce, travel marketplaces, file sharing, financial services, and more – demonstrating that no matter your digital service or platform, GIFCT welcomes your engagement and invites you to join its community.

⁹ <https://gifct.org/membership/>

Hash Sharing

The Hash-Sharing Database

The HSDB is GIFCT's cross-platform database¹⁰ that enables the sharing of "hashes" (or "digital fingerprints") of known terrorist and violent extremist content between member platforms. To facilitate sharing, GIFCT provides a taxonomy that serves as formal guidance for HSDB inclusion. Content found by a member platform is "hashed" in its raw form, ensuring there is no link to any original source platform or user data. Hashes appear as a numerical representation of the original content, making them extremely difficult to reverse-engineer to recreate the original material, and allow for the circulation of information about the content without amplifying it.

Each platform that is part of the HSDB determines its use of and engagement with the database, depending on its own terms of service, how its platform operates, and how it utilizes technical and human resources (among other factors). GIFCT is neither a tech company nor a social media platform and does not own or store any source data or personally identifiable information of any users associated with member platforms. How hashes and the HSDB work is explained below and in an [explainer video](#).¹¹

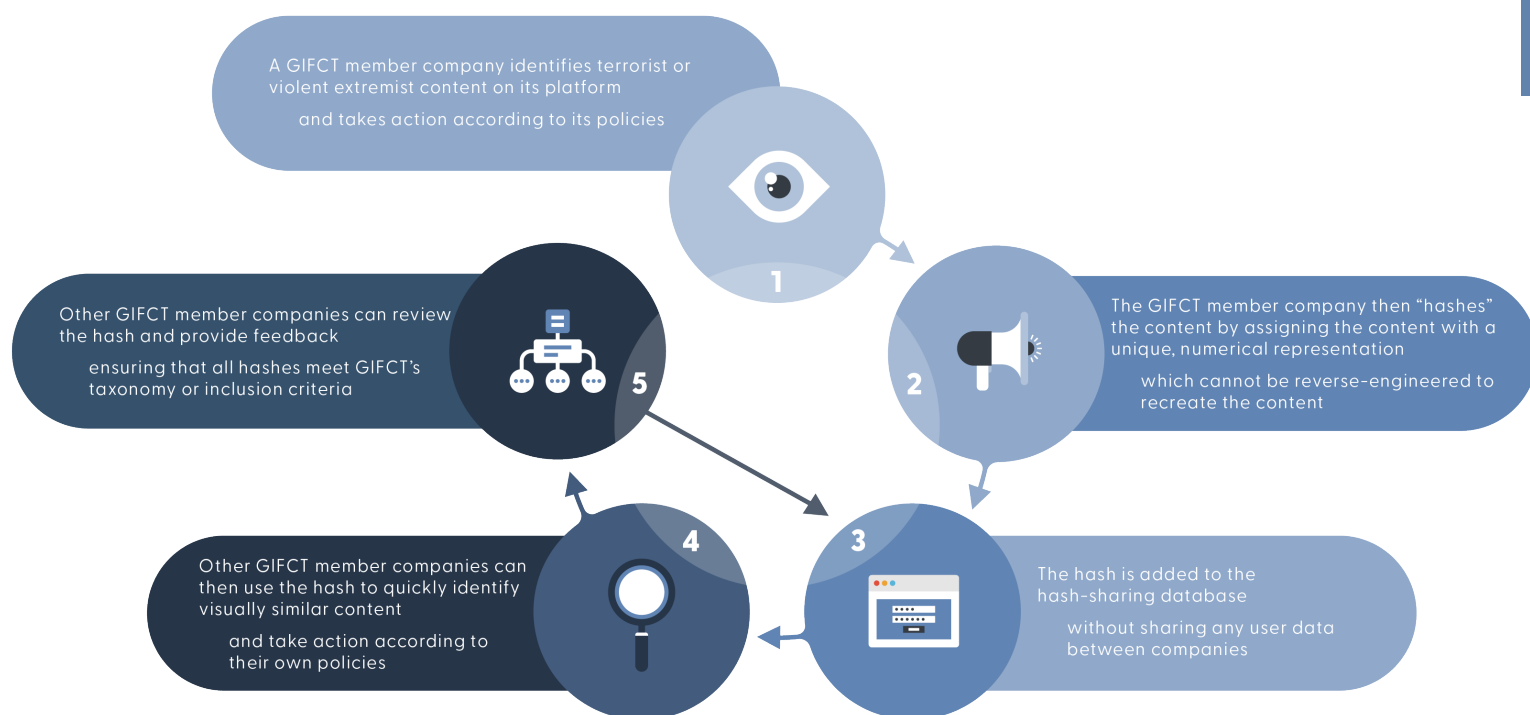


Figure 6: How the HSDB works

Only GIFCT member tech companies have access to the HSDB. Access to the database is provided only to member platforms that have completed its information-sharing agreement, and their use of the database must comply with [GIFCT's HSDB Code of Conduct](#).¹²

¹⁰ <https://gifct.org/hsdb/>

¹¹ <https://gifct.org/hsdb/>

¹² <https://gifct.org/wp-content/uploads/2022/12/GIFCT-Tech-Solution-Code-of-Ethics-GIFCT-For-Publishing-APPROVED-20221115-2.pdf>

Adding hashes does not prompt any direct or automatic action on another member's platform, such as removing content. Each member can use the hashes provided through the HSDB to identify content on their respective platform that matches known terrorist or violent extremist content. Each member also independently determines what potential action to take regarding content on their platform that matches a particular hash, in line with their respective policies and terms of service.

GIFCT members who are integrated into the HSDB (or are in the process of integrating) are primarily focused on user-generated content. These members include Bitly, Dailymotion, Discord, Dropbox, Facebook, Instagram, Giphy, Google, JustPaste.it, LinkedIn, Mailchimp, MEGA, Meta, Microsoft, Niantic, Patreon, Pinterest, Twitch, Vimeo, X, Yahoo, YouTube, Yubo, and Zoom.

Composition of the Hash-Sharing Database

As of the end of 2024, the HSDB contained approximately **2.3 million hashes**. Since the 2023 Transparency Report, members have taken active steps to improve data quality by reviewing and refining the hashes submitted to the HSDB, resulting in a slight reduction in the overall number of hashes in the database and the elimination of hashes deemed no longer needed.

Currently, the HSDB contains approximately **408,000 unique and distinct items, an increase of 38,000 from 2023**, comprising approximately 330,000 visually distinct images, 78,000 visually distinct videos, and 200 textually distinct items related to PDFs.

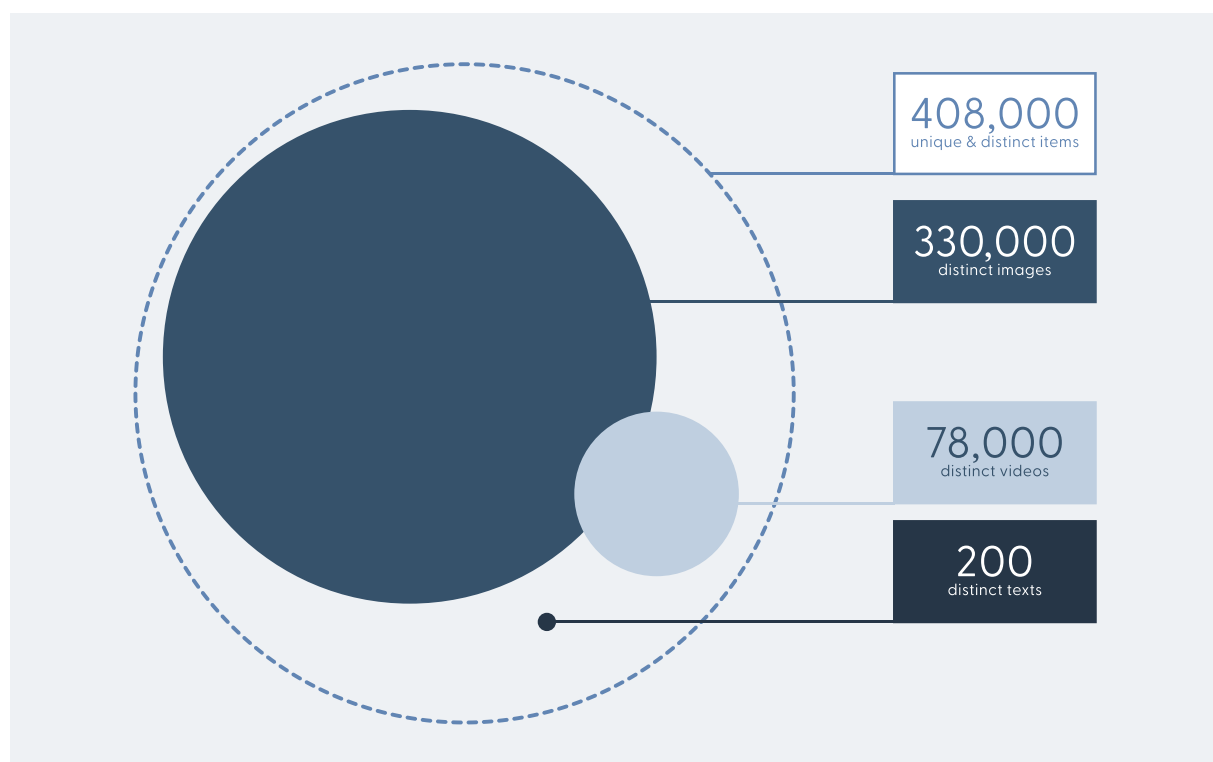


Figure 7: Approximate number of distinct items in the HSDB

Taxonomy for the Hash-Sharing Database

GIFCT has published an updated [taxonomy](#)¹³ as a formal set of parameters for inclusion in the HSDB, reflecting several iterations of input and feedback from a range of stakeholders. Although member companies may have slightly different operational definitions of “terrorism” or “terrorist content,” GIFCT’s taxonomy represents a selection of high-severity content that seeks to capture areas of strong consensus among members.

GIFCT’s taxonomy has evolved from a narrow list-based focus to a more flexible, behavior-based framework developed through multi-stakeholder input. Originally, the taxonomy – and the content in the HSDB – focused strictly on images and videos from entities listed on the [UN Security Council Resolution 1267](#)¹⁴ (Al-Qaida and ISIL) Sanctions List. In 2019, it expanded to include content from perpetrators of offline attacks who live-streamed or recorded their violence, aligning with the IRF.

Following the [2021 Taxonomy Report](#),¹⁵ the scope expanded to include attacker manifestos and branded propaganda materials such as PDFs. Rather than following any single government list, GIFCT now uses a set of criteria that allows for labels referencing designated entities on the 1267 Sanctions List, behavioral labels that categorize content by type, or incident labels created from IRF activations.

Labels for the Hash-Sharing Database

GIFCT maintains a system to provide more information about the reasons for including hashes in the database. In addition to content being linked to a framework based on the UN 1267 Sanctions List, pathways for adding hashes include the following labels:

- **Behavioral labels** categorize hashes by type of terrorist or violent extremist behavior associated with the content.
- **Incident labels** correspond to the offline terrorist or mass violence attack that activated the IRF, which prompts hashing of identified perpetrator-produced content.

Behavioral labels

At the end of 2024, approximately 91% of the total number of hashes in the HSDB included behavioral labels. The majority (75.94%) focused on glorification of terrorist acts, followed by graphic violence related to offline terrorist or violent extremist events (16.65%), terrorist recruitment and instruction (5.27%), and imminent credible terrorist threats (2.14%). Reviews of the HSDB and member user needs are planned for 2025, following the work of the 2024 Working Groups and member and stakeholder feedback.

13 <https://gifct.org/wp-content/uploads/2022/12/HSDB-Taxonomy-FOR-PUBLICATION-Dec-2022-1.pdf>

14 https://main.un.org/securitycouncil/en/sanctions/1267#sanction_measures

15 <https://gifct.org/wp-content/uploads/2021/07/GIFCT-TaxonomyReport-2021.pdf>

Incident labels

GIFCT activated the IRF types that enable hash sharing for the following attacks involving perpetrator-produced content with the following incident labels:

- **Christchurch, New Zealand:** On March 15, 2019, the need for a separate hash label was declared after an attacker live-streamed his attack on two mosques.
- **Halle, Germany:** On October 9, 2019, the Content Incident Protocol (CIP) was activated after an attacker live-streamed his attack on a synagogue.
- **Glendale, Arizona, United States:** On May 20, 2020, the CIP was activated after an attacker live-streamed his attack on the Westgate Entertainment District.
- **Buffalo, New York, United States:** On May 14, 2022, the CIP was activated after an attacker live-streamed his attack on a supermarket.
- **Udaipur, India:** On June 28, 2022, the Content Incident (CI) was activated after the release of a video by attackers showing the killing of an individual.
- **Memphis, Tennessee, United States:** On September 7, 2022, the CIP was activated after an attacker live-streamed his attack on a store as part of a series of attacks throughout Memphis.
- **Louisville, Kentucky, United States:** On April 10, 2023, the CIP was activated after an attacker live-streamed his attack at a bank.
- **Perry, Iowa, United States:** On January 4, 2024, the CIP was activated after an attacker live-streamed his attack on a high school.
- **Levittown, Pennsylvania, United States:** On January 30, 2024, the CIP was activated after a perpetrator live-streamed a violent extremist event.
- **Eskişehir, Türkiye:** On August 12, 2024, the CIP was activated after an attacker live-streamed the stabbing of multiple individuals.
- **Volgograd, Russia:** On August 23, 2024, the CI was activated in response to an ISIS-affiliated killing and hostage incident, and the perpetrator released videos depicting violence associated with the incident.

Of the total number of hashes in the HSDB at the end of 2024, approximately 13% included IRF activation related labels.

Incident Label	Percent of hashes with incident label
Udaipur, India	40.38%
Christchurch, New Zealand	30.68%
Buffalo, New York, U.S.	15.63%
Halle, Germany	10.90%
Memphis, Tennessee, U.S.	1.21%

Eskişehir, Türkiye	0.46%
Volgograd, Russia	0.28%
Levittown, Pennsylvania, U.S.	0.25%
Glendale, Arizona, U.S.	0.19%
Perry, Iowa, U.S.	0.01%
Louisville, Kentucky, U.S.	>0.01%

Table 1: Hash taxonomy incident label distribution

Member Hash Feedback

GIFCT is actively working to improve the quality of the data in the HSDB through member collaboration. This includes a focus on understanding and addressing barriers to participation in hash feedback and other HSDB functions, in line with findings from the 2024 Hash Sharing Working Group (HSWG). Hash feedback – where members can indicate agreement or disagreement with a hash's labeling and inclusion – serves as one such mechanism.

All feedback is visible to GIFCT and participating members, adding valuable context for individual enforcement decisions. As of the end of 2024, approximately 2% of hashes had feedback, with the vast majority of that feedback indicating agreement. GIFCT continues to assess how to better support members in providing feedback and will promote broader collaboration through the HSDB and other shared tools, while also identifying effective metrics to measure progress.

Hash Removals

In some instances, member companies may choose to remove specific hashes from the HSDB. Hashes may be removed for a variety of reasons, such as when a member company conducts automated or human reviews of hashes they have submitted.

Why might a hash be removed?

Individual Platform Review: Members may periodically review and potentially remove hashes they submit to the HSDB to ensure they align with GIFCT's taxonomy.

Member Feedback: Members may choose to review and remove hashes from the HSDB in response to another GIFCT member providing feedback on a hash.

New Information or Evolving Context: Members may reassess hashed content against GIFCT's inclusion criteria in response to changes in how content is used or reappropriated by terrorist or violent extremist groups.

Data Availability: A member may choose to remove hashes if they no longer retain the content corresponding to the hash. Each member platform has a different content retention policy period, but after the period has expired, the original content is no longer retained in compliance with relevant privacy laws.

Reviewing and Refining the Hash-Sharing Database

GIFCT remains committed to gathering input from members and the broader multi-stakeholder community to refine the HSDB and improve the overall quality and impact of all member programs and solutions. Ongoing feedback is essential to ensuring that GIFCT's efforts are responsive to the practical challenges and priorities of its membership.

In 2025, GIFCT will continue to identify opportunities to enhance the HSDB further and implement recommendations from the HSWG. GIFCT is also adopting a forward-looking approach to strengthening the HSDB, including refining inclusion parameters to ensure the database remains aligned with the evolving online threat landscape.

Hash Sharing Working Group

In 2024, GIFCT convened the HSWG to gather critical multi-stakeholder feedback on the HSDB and how it could be improved. Researchers from the National Consortium for the Study of Terrorism and Responses to Terrorism (START) led the HSWG, which included multiple sessions with member platform representatives and experts from six government and civil society organizations.

As a result, the START team led the authorship of a [report](#)¹⁶ reviewing the current status of the HSDB, its use by current GIFCT members, and the overall efficacy of the HSDB and its taxonomy. Through the HSWG and similar initiatives, GIFCT systematically evaluates the effectiveness of its tools and programs, seeking to ensure they meet the evolving needs of its members and the broader counter terrorism and countering violent extremism community.

.....
16 <https://gifct.org/wp-content/uploads/2025/02/GIFCT-24WG-1224-HSDR-Challenges-1.1.pdf>

Incident Response

Incident Response Framework

GIFCT supports its member companies in responding to the online manifestations of offline violence by fostering information sharing and collaboration through the [Incident Response Framework \(IRF\)](#).¹⁷ The IRF is the set of protocols and processes that guide how GIFCT and its members respond quickly, effectively, and in a coordinated manner to terrorist and mass violence events with significant online dimensions. GIFCT employs a centralized communications mechanism as part of its incident-response efforts to share news of ongoing terrorist and mass violence events with members when these events could lead to the spread of violent content produced by perpetrators.

The rapid information sharing that takes place through the IRF allows us to stay ahead of emerging threats and respond in real time. By collaborating with other members and accessing timely intelligence, we have been able to act faster, make informed decisions, and implement safeguards that keep our community and platform safe. We have also been able to provide actionable intelligence to other platforms, allowing us to strengthen one another's responses. This collective effort has become a cornerstone of our safety strategy, and we're proud to contribute to and benefit from such a proactive, united front against harmful content online.

Twitich

Types of Response

GIFCT's IRF contains three responses that reflect the type of online exploitation related to the offline terrorist or violent extremist event, as well as the response GIFCT and its members carry out: Incident, Content Incident (CI), and Content Incident Protocol (CIP). Activating and differentiating between these different responses serves to:

- **increase the speed** at which industry becomes aware of and responds to terrorist and violent extremist content circulating online that relates to an offline terrorist event
- **decrease terrorist and violent extremist content** circulating on digital platforms
- **enhance communications** between industry, government, and civil society in response to a terrorist or violent extremist event

.....
¹⁷ <https://gifct.org/incident-response/>

Activating any IRF response type indicates the heightened threat a situation potentially poses to GIFCT member platforms, including possible exploitation of their digital platforms and GIFCT's urgency in supporting them in stemming the spread of content associated with the incident.

In addition to actively engaging with members during IRF activations, GIFCT also collaborates with relevant government and civil society organizations as well as academia to understand how their insights can further inform GIFCT's continued response.

Since its creation in 2019, **the IRF has been activated 21 times**, representing 11 Incident activations, two CI activations, and eight CIP activations. More information about how the CIP works is available on [GIFCT's website](https://gifct.org/content-incident-protocol/).¹⁸

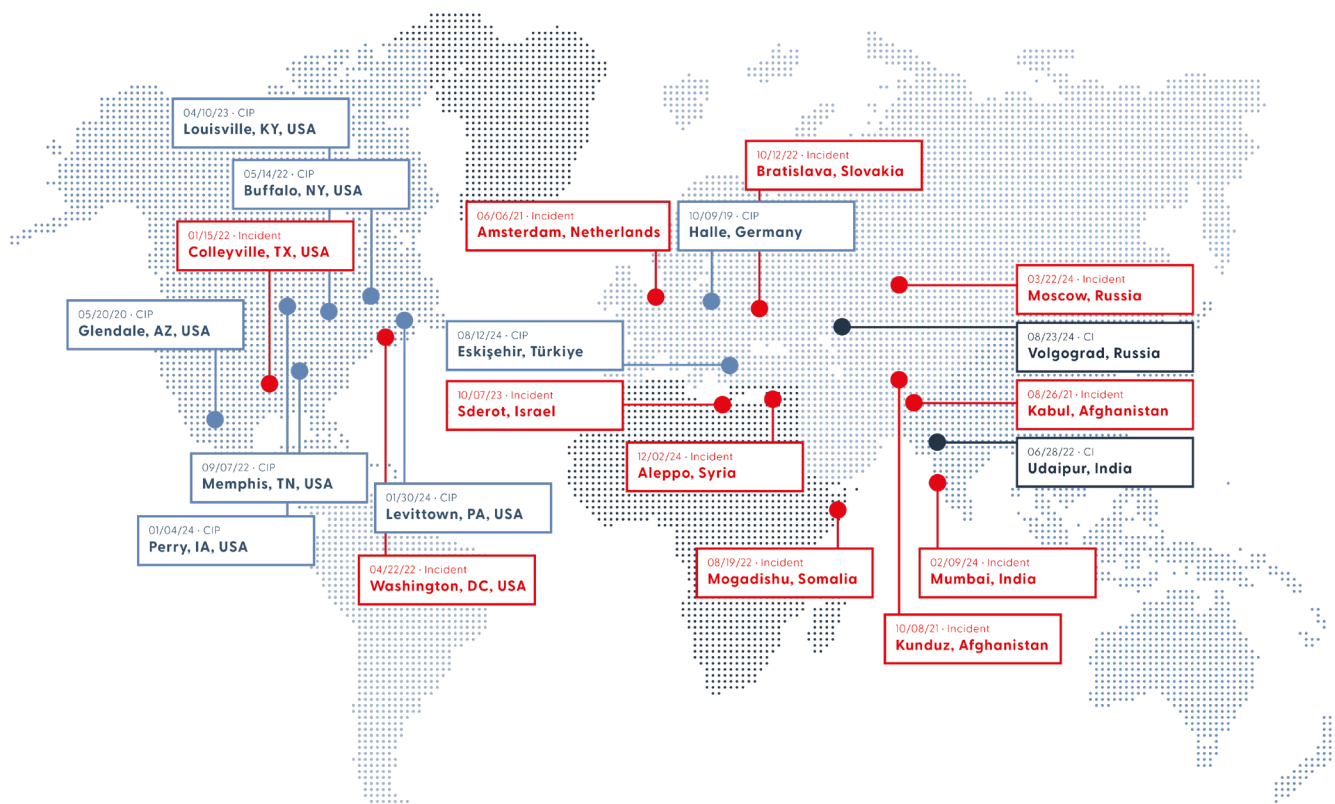


Figure 8: IRF activations by end of 2024

¹⁸ <https://gifct.org/content-incident-protocol/>

2024 Activations

In 2024, GIFCT and its members activated the IRF **seven times**.

When	Location	Activation Type
Jan. 4	Perry, IA, USA ¹⁹	CIP
Jan. 30	Levittown, PA, USA ²⁰	CIP
Feb. 9	Mumbai, India	Incident
Mar. 22	Moscow, Russia	Incident
Aug. 12	Eskişehir, Türkiye ²¹	CIP
Aug. 23	Volgograd, Russia ²²	CI
Dec. 2	Aleppo, Syria	Incident

Table 2: 2024 IRF activations

.....
¹⁹ <https://gifct.org/2024/01/04/content-incident-protocol-perry-iowa/>

²⁰ <https://gifct.org/2024/01/31/content-incident-protocol-levittown-pennsylvania/>

²¹ <https://gifct.org/2024/08/13/incident-response-cip-activated-in-response-to-violent-extremist-event-in-eskisehi-turkiye/>

²² <https://gifct.org/2024/08/23/incident-response-ci-activated-in-response-to-violent-extremist-event-in-volgograd-russia/>

Hashing and the Incident Response Framework

In cases where either a CI or CIP is activated, members can contribute hashes of associated content to the HSDB. The figure below shows the additions of hashes to the database in 2024, categorized by incident. It illustrates the ongoing adversarial nature of continued attempts to share new versions of perpetrator-produced content and evade detection.

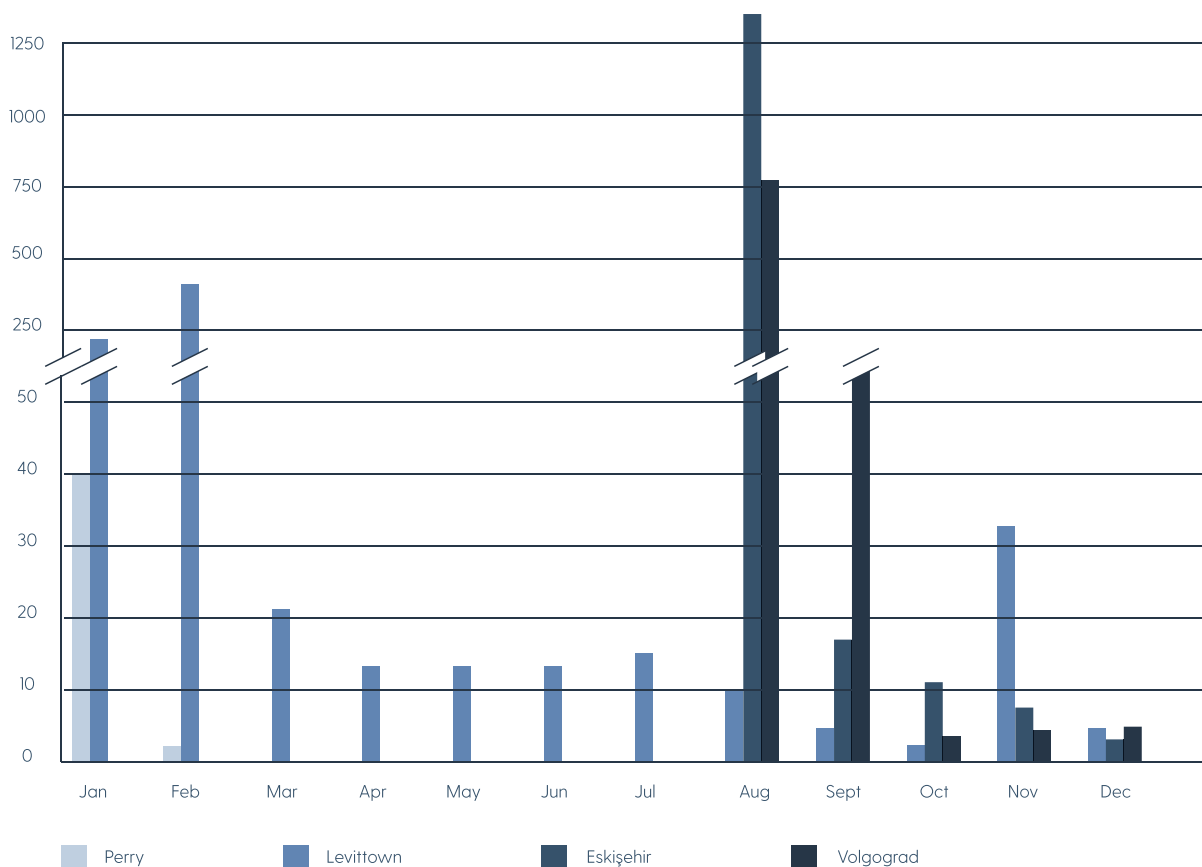


Figure 9: Hashes per Incident, 2024

Reviewing and Refining the Incident Response Framework

In 2024, GIFCT provided more tailored support to members who requested additional analytical assistance or guidance by offering contextual information about online content. This included convening experts and integrating research tools such as Extrac and Open Measures to enhance situational awareness and analytical capacity during incident responses. Members also began to **receive post-incident intelligence bulletins** following activations, which provide insights about the incident, associated ideology or movement, and (when applicable) actionable information for moderation and investigation teams.

GIFCT also continues to host multi-stakeholder debriefs when the CIP is activated, ensuring that stakeholders - including government and civil society actors - are informed of the context and events that prompted the activation of the CIP, as well as the actions carried out as a result.

Incident Response Working Group

In 2024, GIFCT continued to demonstrate its commitment to improving its readiness capabilities and further support members' ability to respond to online harms. One of the most significant developments to come out of 2024 was a collective desire to assess and improve the IRF in its entirety. Informed by [recommendations from the Incident Response Working Group \(IRWG\)](#),²³ GIFCT laid the foundations to conduct a comprehensive review and revamp of the IRF to ensure its protocols remain responsive to the evolving nature of terrorist and violent extremist events.

Research and Analysis

Global Network on Extremism and Technology

GIFCT connects industry members to global expertise and research through its academic arm, the [Global Network on Extremism and Technology \(GNET\)](#).²⁴ Funded and supported by GIFCT, and based at the International Centre for the Study of Radicalisation at King's College London, GNET brings together an international consortium of leading academic institutions and experts to provide GIFCT members and partners with research and analysis on emerging threats and trends, including ongoing crises and conflicts while connecting them to a global network of experts and scholars.

The GNET partnership with GIFCT provides valuable academic research and insight, which informs the work of GIFCT member platforms in combating terrorist and extremist use of their technology. GIFCT's multi-stakeholder approach enables us to connect directly with a range of platforms, allowing us to better understand their needs and concerns. While academic in nature, we produce research that offers pragmatic and clear advice to member platforms on appropriate responses and solutions. We understand that well-informed research is essential to producing active change; GIFCT enables us to ensure all our work is making a real-world impact through industry collaboration.

Dr. Alexander Meleagrou-Hitchens, *Co-director, ICSR and Principal Investigator, GNET*

23 https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-IRWG_Report-1.1.pdf

24 <https://gnet-research.org>



GNET Publications

To foster deeper understanding about global threats, trends, and dynamics, and access to targeted research and findings for consideration by the tech sector, GNET commissions written contributions. The resulting *Insights* are practical analyses of terrorists and violent extremists' exploitation of digital platforms from around the world. In 2024, GNET commissioned over **120 Insights from 111 researchers from 24 countries**, 64 of whom were first time contributors.

Of the published *Insights*, **62 pieces** highlighted attempts by terrorists or violent extremists to exploit GIFCT member platforms specifically, which GIFCT was able to proactively share with the platforms and inform trust and safety efforts.

A selection of the most popular *Insights* from 2024 includes:

- [The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing](#)²⁵ by Animesh Roul
- [Hiding in Plain Sight: How the 'Newgen' Misogynistic Incel Content Creators Escape Moderation on TikTok](#)²⁶ by Anda Solea
- [AI-Powered Jihadist News Broadcasts: A New Trend In Pro-IS Propaganda Production?](#)²⁷ by Federico Borgonovo, Alessandro Bolpagni, and Silvano Rizieri Lucini
- [Melodies of Malice: Understanding How AI Fuels the Creation and Spread of Extremist Music](#)²⁸ by Heron Lopes
- [764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation](#)²⁹ by Marc-André Argentino, Barrett G, and M.B. Tyler

Among these publications, one attracted attention on an Islamist extremist forum, another was featured by the EU Disinformation Lab (which subsequently hosted a webinar to discuss the findings), and a third was presented as evidence in a court case.

GNET produced and published **five reports** and six user journey reports in 2024. GNET reports

25 <https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>

26 <https://gnet-research.org/2024/05/07/hiding-in-plain-sight-how-the-newgen-misogynistic-incele-content-creators-escape-moderation-on-tiktok/>

27 <https://gnet-research.org/2024/05/09/ai-powered-jihadist-news-broadcasts-a-new-trend-in-pro-is-propaganda-production/>

28 <https://gnet-research.org/2024/12/11/melodies-of-malice-understanding-how-ai-fuels-the-creation-and-spread-of-extremist-music/>

29 <https://gnet-research.org/2024/01/19/764-the-intersection-of-terrorism-violent-extremism-and-child-sexual-exploitation/>

provide comprehensive analyses of specific subject matter, while user journey reports examine how individuals enter and participate in online extremist communities. These publications were featured in exclusive launch events that brought together the authors, additional experts, and cross-sector stakeholders for focused online discussions.

Among the reports with the most online engagement were:

- [Transmisogyny, Colonialism and Online Anti-Trans Activism Following Violent Extremist Attacks in the US and EU](#)³⁰ by Anne Craanen, Charley Gleeson, and Anna Meier
- [30 Years of Trends in Terrorist and Extremist Games](#)³¹ by Galen Englund and Emily Thompson
- [White Supremacist and Anti-Government Extremist Groups in the US](#)³² by Katherine Keneally and Jacob Davey
- [The Incel Subculture](#)³³ by the International Centre for the Study of Radicalisation

Microsoft is proud to support GIFCT and its mission to combat terrorism and violent extremism online while upholding fundamental human rights. In a rapidly changing technological and geopolitical landscape, GIFCT plays a unique and essential role – bringing together technology platforms, governments, civil society, and academia to deliver practical, cross-sector solutions. This year's progress reflects the strength of that collaboration, and we look forward to continuing our partnership for the future of online safety.

Courtney Gregoire, Vice President and Chief Digital Safety Officer, Microsoft



30 <https://gnet-research.org/2024/05/24/transmisogyny-colonialism-and-online-anti%20%90trans-activism-following-violent-extremist-attacks-in-the-us-and-eu/>

31 <https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/>

32 <https://gnet-research.org/2024/07/24/white-supremacist-and-anti%20%90government-extremist-groups-in-the-us/>

33 <https://gnet-research.org/2024/07/26/the-incele-subculture/>

GIFCT Knowledge Products

Effective solutions for countering terrorism and violent extremism online must be rooted in a strong understanding of the threat landscape and the context in which they exist. To ensure that members stay informed about significant threats of terrorist and violent extremist exploitation of digital platforms, GIFCT delivers assessments, insights, and bespoke analysis on specific dynamics of the online threat landscape crafted specifically for the needs of its diverse members. GIFCT develops expert analysis and briefings by its in-house experts, publishes research briefs and insights, commissions analysis from GIFCT's network of external experts, and facilitates information sharing between member platforms.

Knowledge products deliver actionable insights and recommendations; some are exclusively for GIFCT members, while others are available to the wider public. This year, in addition to reports, *Insights*, and Working Group publications, GNET (at GIFCT's request) produced member-only threat intelligence products related to major events, significant dates, and regional trends in terrorism and violent extremism. For many of these reports, the authors attended and presented their findings during GIFCT monthly member meetings. Among the knowledge products produced in 2024 were:

- [“Horizon Scanning: The Future of Counterspeech and Positive Interventions”](#)³⁴ by Dr. Erin Saltman and Munir Zamir, published as an insight from a co-authored chapter in the book *Counterspeech: Multidisciplinary Perspectives on Countering Dangerous Speech*.
- [“Human Rights-Based Approaches to Preventing Terrorists and Violent Extremists from Exploiting Digital Platforms”](#)³⁵ which draws on the human rights virtual roundtable convened by GIFCT with BSR, focusing on human rights considerations for tech companies with regard to countering terrorism and violent extremism.
- [“Resolution 2734: What the Update to the UN Sanctions Regime Means for Tackling Terrorist Use of Sexual Violence”](#)³⁶ by Naureen Chowdhury Fink and Cyndee Trinh, published by the International Peace Institute's *Global Observatory*.

In addition to these knowledge products, GIFCT kept members engaged and informed by convening ad-hoc, member-only events and activations, often tailored to specific member needs.

.....
³⁴ <https://gifct.org/2024/02/28/the-future-of-counterspeech/>

³⁵ <https://gifct.org/2024/04/22/human-rights-based-approaches/>

³⁶ <https://theglobalobservatory.org/2024/11/resolution-2734-what-the-update-to-the-un-sanctions-regime-means-for-tackling-terrorist-use-of-sexual-violence/>

Knowledge Exchange and Collaboration Events

Bringing together key stakeholders from industry, government, civil society, and academia through events such as workshops, conferences, and roundtables plays a critical role in enabling GIFCT to foster a deeper understanding of global trends and dynamics. Throughout 2024, GIFCT organized **five GIFCT-sponsored events** that facilitated knowledge exchange, promoted collaboration, and supported members in adapting to the ever-evolving online threat landscape. GIFCT also supported **GNET's fourth annual conference** and the webinars it produced in 2024. Through these interactions, GIFCT produces targeted knowledge products and resources that advance collective understanding and equip members to navigate the complexities of online and offline threats from terrorists and violent extremists.



Global Multi-Stakeholder Forum

In June, GIFCT and the 2024 Operating Board Chair, Microsoft, hosted a [Global Multi-Stakeholder Forum](https://gifct.org/2024/07/16/gifct-hosts-2024-multistakeholder-forum-in-singapore/)³⁷ in Singapore, bringing together members, experts, practitioners, and international representatives from civil society and government.



.....
³⁷ <https://gifct.org/2024/07/16/gifct-hosts-2024-multistakeholder-forum-in-singapore/>

Following opening remarks from Singapore's Minister for Home Affairs and Minister for Law K. Shanmugam, sessions addressed regional terrorism threats and challenges, the implications of and opportunities associated with using AI to counter terrorism, and strategies for mitigating risk effectively.

Through these discussions and collaborations, GIFCT gained new insights to inform its work on identifying and delivering cross-platform solutions for members, explored new developments in the threat landscape, and deepened its understanding of regional and international dynamics and best practices to address online harms and their offline impacts across the world.



Regional Workshops

Workshops have been a core part of GIFCT's work since its establishment, serving as critical opportunities to build global partnerships, identify prospective members, and ensure that GIFCT's activities are informed and shaped by a range of global perspectives and experiences.

Firjan was honored to host the LatAm Tech Workshop with GIFCT at Casa Firjan, our innovation think tank in Rio de Janeiro. Hosting such a relevant event—one that promotes dialogue among key sectors in the fight against cyberterrorism and radicalization online—reinforces our commitment to innovation in service of safety and society.

Collaboration among governments, tech companies, academia, and civil society is essential to strengthening digital resilience and developing effective solutions to emerging threats. Like GIFCT, we believe that knowledge sharing and the exchange of experiences are indispensable paths toward building a safer digital environment, free from violent extremism.

Firjan remains committed to partnerships, like this one with GIFCT, that bring together intelligence, technology, and social responsibility in pursuit of a safer and more connected future.

Industry Federation of the State of Rio de Janeiro (Firjan)

In 2024, GIFCT hosted workshops located in Rio de Janeiro, Brazil and Stockholm, Sweden. The [LatAm Tech Workshop](#),³⁸ in partnership with Firjan, marked GIFCT's first engagement in Latin America. The event connected industry leaders, tech platforms, and experts, offering valuable insights into regional digital trends and global counter terrorism efforts.

The Latin American workshop organized by GIFCT in Rio served as a powerful reminder of the importance of collaborative spaces in building resilience against terrorism and violent extremism online. As a platform that prioritizes safety-by-design, Yubo recognizes the crucial value of engaging in transparent, cross-sector conversations that unite policymakers, intelligence agencies, civil society, and other tech platforms.

Collaborating with institutions such as Brazil's Intelligence Agency and the UN Counter-Terrorism Committee Executive Directorate (CTED) was an enriching opportunity to discuss the evolving threat landscape in South America and worldwide, particularly given increasingly interconnected online spaces. This collaboration enabled us to stay abreast of practical preventive strategies rooted in real-world insights. GIFCT continues to play a vital role in shaping our understanding and enhancing our ability to respond promptly and responsibly. We take pride in being part of a network that emphasizes knowledge-sharing, accountability, and proactive measures.

Lucas Gagliardi, *Policy Manager, Yubo*

.....
 38 <https://gifct.org/2024/04/29/latam-tech-workshop/>

Later in the year, GIFCT partnered with Nordic Safe Cities in co-hosting tech-focused sessions and a [multi-stakeholder workshop during the Nordic Democracy Forum](#),³⁹ which brought together over 200 participants, including regional ministers, national and local leaders, practitioners, academics, civil society representatives, tech platforms, foundations, and youth organizations.

At the Nordic Democracy Forum, GIFCT played a key role in bringing leading tech companies into vital conversations about safeguarding democratic values in the digital sphere with key actors from civil society, research, and politics. Their contribution helped enable a unique, closed-door workshop where cities, platforms, and governments could explore shared challenges and co-develop forward-looking, cross-sector solutions to extremism and online threats.

Nordic Safe Cities



Canada Center Mega Week

In May of 2024, Executive Director Naureen C. Fink and Membership and Programs Senior Lead Nagham El Karhili were pleased to join senior practitioners, subject matter experts, and policymakers for the fifth international “Mega Week” conference in Montreal hosted by Public Safety Canada’s Canada Centre for Community Engagement and Prevention of Violence.

The meetings provided invaluable opportunities to learn from frontline practitioners, civil society organizations, industry, and government about lessons learned, good practices, and experiences mitigating terrorism and violent extremism, both offline and online.

.....
 39 <https://gifct.org/2024/11/21/gifct-partnership-in-the-nordic-democracy-forum-in-stockholm/>

External Engagements

To date, GIFCT has engaged with a diversity of tech platforms, NGOs, and government bodies through its workshops and activations across the globe. In addition to GIFCT-hosted events, GIFCT senior experts regularly participate in international workshops and events to foster knowledge exchange and engagement with GIFCT resources and to identify new members and partners.

In May 2024, for example, Executive Director Naureen C. Fink was the Key Note speaker at a conference organized by the Organization for Security and Cooperation in Europe (OSCE) and the Government of Mongolia, with support from the U.S. State Department, focused on “Addressing the Prevailing Digital Information Disorder: Countering the Use of the Internet by Terrorists & Violent Extremists.”



Additionally, in October 2024, Director of Memberships and Programs Dr. Erin Saltman briefed senior officials and practitioners at Interpol's headquarters in Lyon for the Expert Level Meeting on Synergies between Law Enforcement, Intelligence and Tech Companies in Countering Terrorism hosted by the Aqaba Process. GIFCT briefed on the current state of play with online terrorist and violent extremist threats and also led attendees in a Table-Top Exercise to better understand incident response processes and multi-stakeholder protocols.

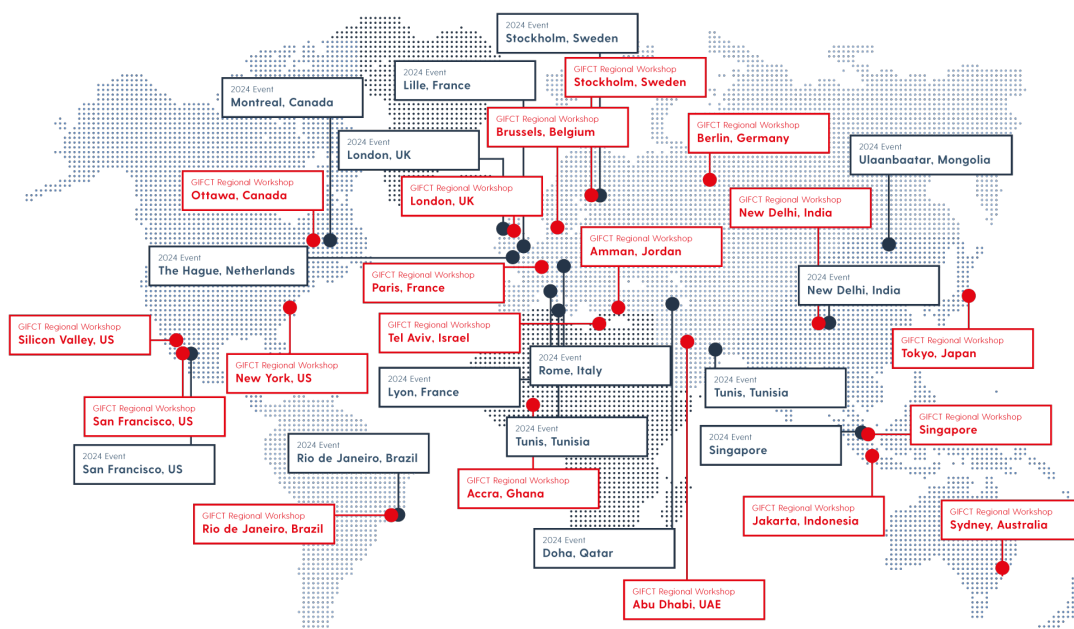


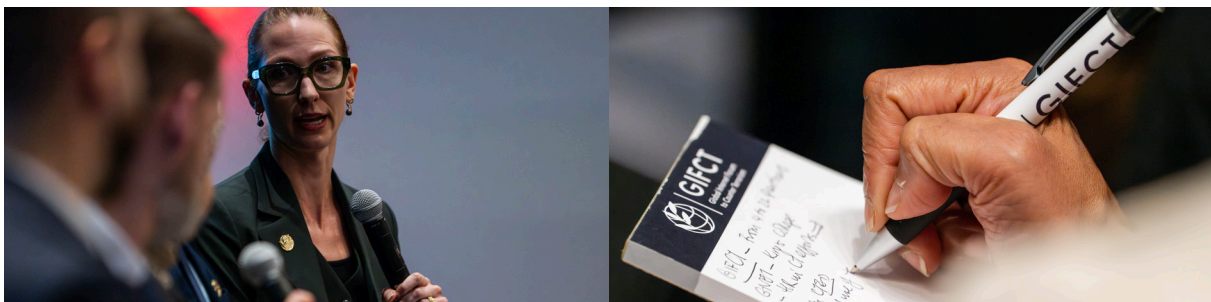
Figure 10: GIFCT Regional Workshops and 2024 events



United Nations, New York

On the margins of the opening of the 79th United Nations General Assembly session (UNGA) in September 2024, GIFCT co-hosted with the UN Security Council CTED [a multi-stakeholder event](#)⁴⁰ bringing together representatives from industry, civil society, academia, and senior government officials focused on the impacts and implications of emerging technologies for international counter terrorism efforts. The event underscored the need for collective action to address emerging technologies such as generative AI and drones, and stressed the importance of understanding regional contexts, upholding human rights, and strengthening global partnerships to effectively address these challenges.

Additionally, GIFCT co-hosted two roundtables with Meta: one on the intersections of sanctions and counter terrorism in the tech sector, and another on strategies for building resilience through youth-focused online prevention efforts. These events brought together both long-standing members of GIFCT's network and new partners, reinforcing GIFCT's position as a leading convener and trusted voice in the global counter terrorism landscape.



2024 Annual Member Forum

In partnership with its 2024 Board Chair, Microsoft, GIFCT hosted its **Annual Member Forum** – a milestone event following a series of governance updates adopted by the Operating Board in the summer, and offering members an opportunity for intra-network dialogue and collaboration and access to insights from the IAC on threats and trends. Following the governance changes, this meeting provided a critical opportunity for participants to engage directly with the Operating Board and help shape GIFCT's strategic priorities for 2025. The closed-door format allowed for candid discussions on platform-specific interests and priorities to inform GIFCT's 2025 planning and activities, and fostered greater member engagement in developing GIFCT priorities.

.....
 40 <https://gifct.org/2024/10/08/news-gifct-side-events-at-the-79th-unga-emerging-technologies-counterterrorism-sanctions-and-youth-pve-initiatives/>



GNET Conference

The fourth annual **GNET Conference** was held in London on May 29th and 30th at King's College London. The event provided a critical opportunity for researchers and industry professionals to meet in person. Through a series of panel sessions spread across two days, participants covered global trends in the online threat landscape, AI and violent extremism, emerging technologies, extremism and elections, and gaming and radicalization.

GNET Webinars

In 2024, GNET hosted **seven webinars** exploring trends in terrorist exploitation of the internet and online counter terrorism responses. Over the course of the 2024 webinar series, GIFCT and GNET convened over **1,000 participants** from academia, government, civil society, tech, intergovernmental organizations, policy, intelligence, and law enforcement.

Topics included:

- Artificial Intelligence and Violent Extremism: Ethical Approaches and Counter Measures
- Digital Battlegrounds: Countering Radicalisation on Gaming(-adjacent) Platforms
- Extremism and Emerging & Disruptive Technologies (EDT): Complexities and Containment
- Elections and Extremism: Trends, Consequences and Mitigating Measures
- Extremism and Technology: Emerging Trends from the Global South

2024 Working Groups

In May 2024, GIFCT launched its **Year 4 Working Groups**⁴¹ to facilitate dialogue, foster understanding, and produce outputs to directly support its mission of preventing terrorists and violent extremists from exploiting digital platforms across a range of sectors, geographies, and disciplines.

The three 2024 Working Groups convened over **145 participants** from **32 countries**, with approximately **half drawn from civil society** (12% advocacy, 21% academia, and 18% practitioners), **23% representing governments**, and **26% in tech**.

.....
⁴¹ <https://gifct.org/year-four-working-groups/>

Participants of GIFCT Working Groups represented a range of organizations and platforms, including:

Category	Affiliation
Tech Industry	ExTrac AI Memetica Meta SpaceYaTech Discord Inc GoDaddy.com, LLC SoundCloud Microsoft Niantic Labs Insikt AI Dataietica.org Mozilla Corporation Xbox X (formerly Twitter) Yubo ISACA Kenya Resolver TikTok Amazon Web Services (AWS) Twitch YouTube Dropbox Nexi Group Polygraf AI Fem AI
Government and Intergovernmental Organizations	Department of Home Affairs, Countering Violent Extremism Branch, Online Terrorism & Violent Extremism Policy Section, Australia Federal Bureau of Investigation (FBI), United States of America Virginia State Police, United States of America Department of State, United States of America Ministry of Justice and Security, the Netherlands Australia eSafety European Commission Te Mana Whakaatu – Classification Office (New Zealand Office of Film and Literature Classification) United Nations Counter-Terrorism Executive Directorate (CTED) Federal Ministry of the Interior and Community, Germany Home Office, United Kingdom United Nations Office of Counter Terrorism (UNOCT) Public Safety Canada Organization for Security and Co-operation in Europe (OSCE), Action against Terrorism Unit United Nations Interregional Crime and Justice Research Institute (UNICRI) U.S. Department of Homeland Security Center for Prevention Programs and Partnerships Aqaba Process, Government of Jordan United Nations Counter-Terrorism Centre (UNCCT), Global P/CVE Programme UK Office of Communications (Ofcom)

Practitioners	<p> Moonshot Hedayah Tremau Centinel The Millennium Project (South Asia Foresight Network) [SAFN] Global Disinformation Index Peace Research Institute Frankfurt (PRIF) The Investigative Project on Terrorism Infobae Militant Wire Online Safety Exchange Digital Security Group Jihadoscope Tech Against Terrorism Brookings Institution </p>
Civil Society	<p> ARTICLE 19 Internet Society Anti-Defamation League (ADL) Policy Center for the New South Search for Common Ground Institute for Strategic Dialogue (ISD) ASEAN Coalition to Stop Digital Dictatorship Christchurch Call KızBaşına (Just-a-Girl) All Tech is Human (ATIH) Extremism and Gaming Research Network (EGRN) Southern Poverty Law Center Association of British Muslims Take This Koan Advisory </p>
Academia	<p> Academic Council on the United Nations System (ACUNS) Swansea University Sapienza University of Rome University of Cambridge Columbia University School of International and Public Affairs (SIPA) University of Essex, Department of Government Central University of Gujarat University of Paris Cité Royal United Services Institute (RUSI) University of Waterloo Trinity College Dublin American University Georgia State University The University of Cincinnati, Center for Cyber Strategy & Policy, School of Public and International Affairs Collaboratory Against Hate, Carnegie Mellon University and University of Pittsburgh Macquarie University University of South Wales University of Sussex University of London Georgetown University Hessian University of Public Management and Security </p>

Table 3: List of Year 4 Working Group participant affiliations

The 2024 GIFCT Working Groups focused on the following three topics:

Hash Sharing: This group reviewed GIFCT's HSDB inclusion criteria and proposed enhancements to improve its transparency and accuracy. The National Consortium for the Study of Terrorism and Responses to Terrorism (START) worked with GIFCT to produce a [set of concrete recommendations](#)⁴² for enhancing transparency and accuracy in the HSDB. GIFCT will be implementing recommendations for enhancing transparency and accuracy in the HSDB throughout 2025 to ensure the database remains effective and impactful in cross-platform counter terrorism efforts.

Incident Response: In 2024, GIFCT conducted a robust multi-stakeholder review of its IRF to better reflect the needs and feedback of key stakeholders and draw on lessons learned from prior activations. Widespread concerns about the potential rise in AI-generated content around terrorist attacks and the increasing prevalence of violence associated with accelerationist movements or self-mobilized radicalization informed discussions aimed at updating the IRF. Working with the Center on Terrorism, Extremism, and Counterterrorism (CTEC), GIFCT undertook a comprehensive review and expert dialogue series, which resulted in a [published report](#)⁴³ that will inform GIFCT's work in updating the IRF in 2025.

Gaming: The Gaming Community of Practice (GCoP) was formed to foster collaboration, knowledge sharing, and innovation among practitioners in the gaming industry alongside global experts. The group aimed to inform the development of best practices and guidance to prevent terrorists and violent extremists from exploiting games, gaming-adjacent services, and the gaming community. Leading members of the Extremism and Gaming Research Network (EGRN) produced a series of outputs based on Working Group meetings to guide online gaming platforms in developing greater awareness of terrorist and violent extremist threats and how to counter them. The GCoP Working Group outputs included:

- [Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces](#)⁴⁴
- [2024 Resource List: Violent Extremism, Radicalization, and Gaming](#)⁴⁵
- [Threat Surfaces in Games: Challenges and Best Practices](#)⁴⁶

Industry actors within the group also explored how to expand the evolution of threat and signal sharing, which will remain a focus for GIFCT's Investigators' Community of Practice Working Group in 2025.

These multi-stakeholder engagements and the findings they produce are crucial to helping GIFCT improve the resources, tools, and solutions it provides to its members. GIFCT is grateful to all participants for their valuable contributions toward its shared mission.

42 <https://gifct.org/wp-content/uploads/2025/02/GIFCT-24WG-I224-HSDR-Challenges-1.1.pdf>

43 https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-IRWG_Report-1.1.pdf

44 <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>

45 <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>

46 <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-Threat-Surfaces-1.1.pdf>

Human Rights

Promoting and protecting human rights is central to GIFCT's mission to prevent terrorist and violent extremist exploitation of digital platforms. In 2020, its first year operating as an independent organization, GIFCT sought advice from a diverse range of global stakeholders on how best to proactively incorporate human rights considerations into its work. In 2021, GIFCT published a [Human Rights Impact Assessment](#),⁴⁷ making transparent a set of guidelines to ground GIFCT's work in the UN Guiding Principles on Business and Human Rights.

The subsequent [Human Rights Policy](#)⁴⁸ adopted by GIFCT notes that "[t]he participation of both governments and platforms in GIFCT means that both the state duty to protect human rights and the corporate responsibility to respect human rights have direct relevance to our work." The assessment remains a valuable resource that informs GIFCT's ongoing dialogue with current and incoming members as well as stakeholders in industry, government, and civil society.

2024 Developments

In 2024, GIFCT deepened its commitment to human rights by ensuring that across its work, it engaged a diversity of perspectives and expertise, considered the impacts on fundamental freedoms, and identified ways to strengthen its commitment. In 2024, GIFCT:

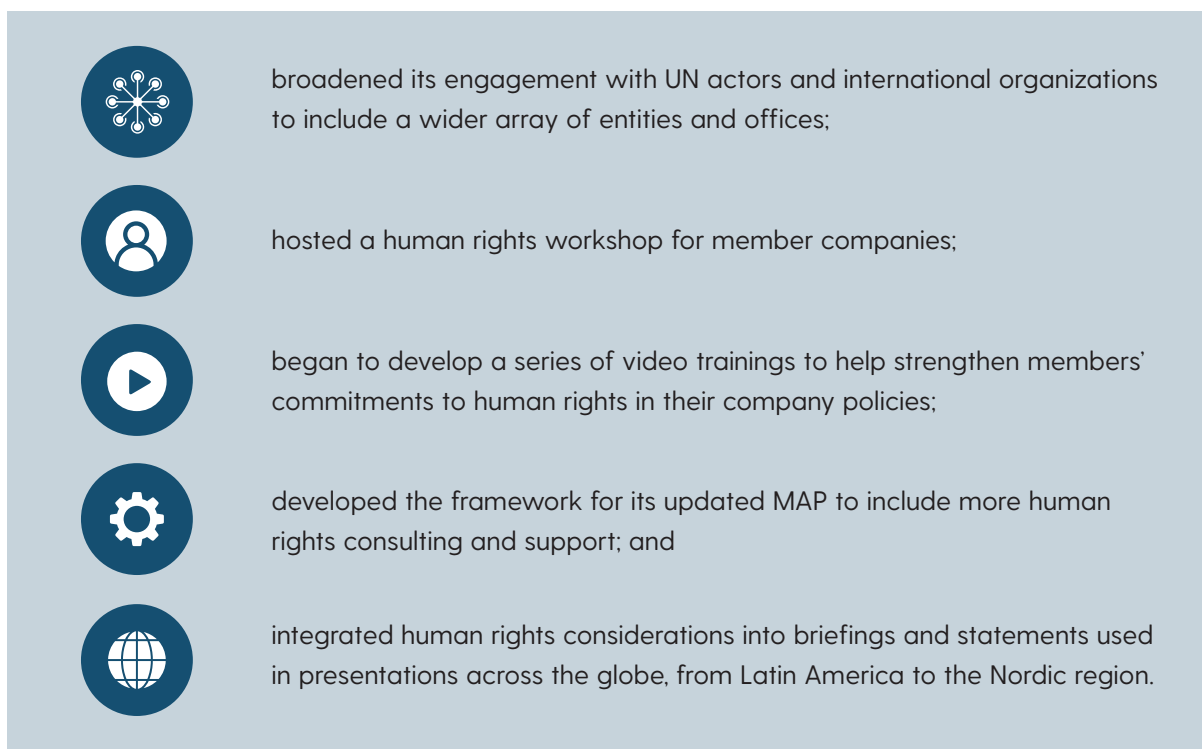


Figure 11: 2024 GIFCT human rights developments

47 https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf

48 <https://gifct.org/wp-content/uploads/2022/12/GIFCT-HumanRightsPolicy-13.12Update.pdf>

Our partnership with GIFCT continues to evolve in support of the organization's long-term human rights goals and expanding membership. In 2024, we broadened our collaboration to include a new suite of trainings, events, and resources designed to help prospective and current members strengthen their human rights policies. As GIFCT takes on a more active role in the membership advisory process, we look forward to continuing this work and supporting GIFCT and its members in implementing their commitments to human rights.

Lindsey Andersen, Associate Director, Tech and Human Rights, BSR

Financials

Financial Support and Contributions

At the end of 2021, GIFCT introduced a tiered membership donation framework to expand financial contributions beyond its four founding member platforms, offering suggested contribution levels based on company revenue. GIFCT is working with the Operating Board on further financial diversification and implementing agreed-upon principles for development efforts.

In 2024, GIFCT's member contributions totaled **\$3,207,500**












Tier	GIFCT Members
Leadership Level >\$750,000	 Meta  Microsoft  YouTube
General Member <\$750,000 (Voluntary Contributions)	 airbnb  amazon  BITCHUTE  DISCORD  Dropbox  Pinterest  zoom 

Table 4: Leadership contributions and voluntary member contributions

GIFCT is grateful to its members for their commitment to its mission and their continued support. These contributions enable GIFCT to sustain, grow, and enhance the technical solutions, tools, and resources it provides to its members and partners, thereby deepening engagement and support within its global, multi-stakeholder community.

2024 Expenses

GIFCT 2024 expenses, totaling **\$3,305,731**, break down as follows:

Category	Total
Administration and Operations	\$967,692
Programming and Delivery	\$2,276,965
Development	\$61,074

Table 5: 2024 expenses by category

As GIFCT continues to grow its membership and expand its reach, the technical solutions, tools, and resources that it provides to members and develops in partnership with its multi-stakeholder network play an especially critical role in the organization's operations. In 2024, GIFCT's suite of programming and delivery tools included facilitating its Working Groups, hosting the Global Multi-Stakeholder Forum, producing an event alongside the UN General Assembly, producing regional workshops, supporting GNET, and overseeing the IRF and the HSDB. Delivering these programs empowers GIFCT with an enhanced understanding of regional trends and dynamics both online and offline, which improves the resources, tools, and solutions provided to both member tech platforms and multi-sector stakeholders alike. The chart below represents the various member programs and solutions that GIFCT provides within the Programming and Delivery budget category.

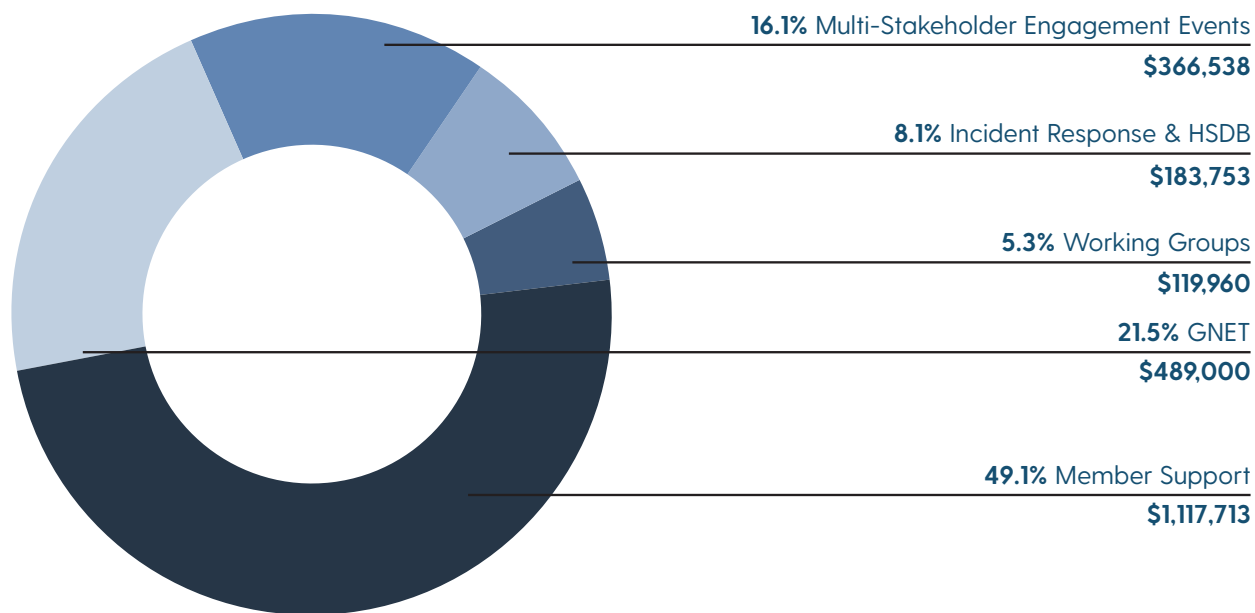


Figure 12: Programming and Delivery

In addition to investing in programming and delivery, GIFCT remains committed to sustainable growth by actively pursuing diverse fundraising opportunities to support its long-term mission. To ensure a strong foundation for this work, GIFCT allocates resources to cover essential administrative and operational costs. This includes supporting staff, maintaining effective systems, building the organizational capacity needed to deliver impact at scale, and identifying and cultivating strategic development opportunities.

Improving GIFCT's Readiness in 2025

Looking forward to 2025, GIFCT remains focused on strengthening its efforts to deliver on its mission of preventing terrorists and violent extremists from exploiting digital platforms. In mid-2024, its Operating Board adopted the [2025–2027 Strategic Plan](#)⁴⁹ developed by GIFCT, and with inputs from the IAC, to support and strengthen its community, and enhance the capacity and capability of the tech industry and its partners. The year ahead will mark a period of strategic growth, operational enhancements, and deeper global collaboration.

In alignment with the new 2025–2027 Strategic Plan, GIFCT is enhancing its support structures, refining its tools, and strengthening its multi-stakeholder model to ensure that its community is equipped to respond to an increasingly dynamic threat environment. Central to this will be the **launch of the MAP in 2025**, which will offer tailored support to prospective and candidate tech companies as they work towards GIFCT membership. By integrating the mentorship program into the MAP, GIFCT will implement streamlined processes that provide its members with more direct access to the technical solutions, tools, and resources they rely on.

Supporting and strengthening a collaborative tech-led multi-stakeholder community remains a core priority. In 2025, GIFCT will undertake a **comprehensive review and revision of the IRF**, drawing on feedback from the IRWG and prior IRF activations. This effort will ensure that the framework remains responsive to member needs and continues to evolve in line with real-world developments. Similarly, GIFCT will implement key recommendations from its HSWG to **improve the effectiveness and utility of the HSDB**, reinforcing its role as a vital tool in limiting the spread of terrorist and violent extremist content online.

Looking ahead, GIFCT will deepen its focus on enhancing the collective capacity of the tech industry and its partners. This includes **fostering a broader and more diverse community** of member companies that reflects the evolving threat landscape. As GIFCT grows its membership, it remains committed to inclusivity across company size, geography, and technological focus.

GIFCT also recognizes the continued importance of **integrating human rights** considerations into all aspects of its work and implementing the recommendations in the Human Rights Impact Assessment commissioned in 2021. In 2025, GIFCT will further strengthen its human rights efforts by delivering more explicit guidance and dedicated support to members as they refine their policies and practices and deepen their understanding of the implications of terrorism and counter terrorism efforts on human rights. This work will involve a comprehensive reassessment of how GIFCT's tools and solutions intersect with human rights standards and practices, ensuring that its collective efforts are both effective and rights-respecting.

As new threats emerge and technologies evolve, GIFCT's work in 2025 will be guided by industry innovations and solutions, cross-sector collaboration, the feedback it has received and the opportunities identified for improvement, and its unwavering commitment to upholding human rights. Together with its members and partners, **GIFCT remains dedicated to improving online safety for all.**

.....
 49 <https://gifct.org/2024/08/15/gifct-strategic-plan-2025-2027-adopted/>

Copyright © Global Internet Forum to Counter Terrorism 2025

Recommended citation: *2024 GIFCT Annual and Transparency Report*. Washington, D.C.: Global Internet Forum to Counter Terrorism, 2025.

GIFCT is a 501(c)(3) non-profit organization and tech-led initiative with over 30 member tech companies offering unique settings for diverse stakeholders to identify and solve the most complex global challenges at the intersection of terrorism and technology. GIFCT's mission is to prevent terrorists and violent extremists (TVE) from exploiting digital platforms through our vision of a world in which the technology sector marshals its collective creativity and capacity to render TVE ineffective online. In every aspect of our work, we aim to be transparent, inclusive, and respectful of the fundamental and universal human rights that TVE seek to undermine.



www.gifct.org



outreach@gifct.org